Elaine A. Ryan (AZ Bar No. 012870)
Colleen M. Auer (AZ Bar No. 014637)
AUER RYAN, P.C.
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139
(520) 705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com

Jean S. Martin* (NC Bar. No. 25703)
Francesca K. Burne* (FL Bar No. 1021991)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 559-4908
Fax: (813) 222-4795
jeanmartin@forthepeople.com
fburne@forthepeople.com

*to seek Admission *Pro Hac Vice*

Attorneys for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Charles Peterson, individually and on behalf of all similarly situated persons, Plaintiff, v. Medical Management Resource Group, LLC d/b/a American Vision Partners, Defendant.	No. **CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF** Jury Trial Demanded

Plaintiff CHARLES PETERSON ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant MEDICAL MANAGEMENT RESOURCE GROUP, LLC d/b/a AMERICAN VISION PARTNERS ("Defendant"), an Arizona company, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") at MMRG, a healthcare-focused company that provides administrative, management, and technology services. As a result of the Data Breach, Plaintiff and approximately 2.4 million Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant for safe keeping —was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes names, contact information, dates of birth, certain medical information (e.g., services received, clinical records, and medications), and Social Security numbers and insurance information. The Data Breach included protected health information ("PHI") as defined by the Health

Insurance Portability and Accountability Act of 1996 ("HIPAA"), and personally identifiable information ("PII") that Defendant collected and maintained (collectively "Private Information").

4. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

5. Defendant collected and maintained Private Information in a reckless manner.

6. In particular, Private Information was collected by Defendant and maintained on its computer network in a condition vulnerable to cyberattacks.

7. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored Private Information, it would have discovered the intrusion sooner.

9. Plaintiff's and Class Members' identities are now at increased risk of identity theft because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

15. Plaintiff CHARLES PETERSON is, and at all times mentioned herein was, an individual citizen of the State of Arizona. Plaintiff is a patient who received health care services from one of Defendant's customers. Plaintiff was sent and received a Breach Notification letter.

16. Defendant MEDICAL MANAGEMENT RESOURCE GROUP, LLC d/b/a AMERICAN VISION PARTNERS is a company that provides healthcare-focused management, administrative, and technology services with its principal place of business in 2121 E. Rio Salado Parkway, Ste 220, Tempe, Arizona 85281.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

18. This Court has personal jurisdiction over Defendant because Defendant has availed itself of the rights and benefits of the State of Arizona by engaging in activities

including (i) directly and/or through its parent companies, affiliates and/or agents providing services throughout the United States in this judicial district and abroad; (ii) conducting substantial business in this forum; (iii) having a registered agent to accept service of process in the State of Arizona; and/or (iv) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in Arizona and in this judicial District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District of Arizona.

DEFENDANT's BUSINESS

20. Defendant is a company that provides healthcare-focused management, administration, and technology services to ophthalmology practices.[1]

21. In the ordinary course of providing its services to customers which are generally healthcare providers, customers provide to Defendant access to their patient data,[2] such as:

- Names;
- Dates of birth;
- Social Security numbers;

---

[1] *Hack at Services Firm Hits 2.4 Million Eye Doctor Patients*, BankInfo Security (Feb. 21, 2024), https://www.bankinfosecurity.com/hack-at-services-firm-hits-24-million-eye-doctor-patients-a-24418.

[2] *MMRG Notifies Patients of Cybersecurity Incident, Business Wire* (Feb. 6, 2024), https://www.businesswire.com/news/beverlyhillschamber/20240206060527/en.

- Driver's license numbers;
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Beneficiary information;
- Provider information;
- Address, phone number, and email address, and;
- Health insurance information.

22. As a condition of receiving healthcare administration services, Defendant requires that its customers entrust it with highly sensitive personal information.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

24. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

25. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

/ / / /

/ / / /

/ / / /

/ / / /

THE CYBERATTACK AND DATA BREACH

26. On or about February 6, 2024, Defendant for the first time publicly announced the Data Breach.[3]

27. According to Defendant, on November 14, 2023, Defendant became aware of a possible cybersecurity incident affecting its systems. Defendant launched an investigation, retaining third-party cybersecurity vendors to assist with the investigation.[4]

28. On December 6, 2023, Defendant concluded that, on November 14, 2023, "[an] unauthorized party obtained personal information associated with patients of the relevant practices[] [serviced by Defendant.]"[5]

29. Defendant determined that the following types of information potentially compromised from the Data Breach include, but are not limited to: "names, contact information, dates of birth, certain medical information (e.g., services received, clinical records, and medications), and in certain cases, Social Security numbers and insurance information."[6]

---

[3] *Id.*; *see also Breach Portal*, U.S. Dep't of Health and Human Servs. Off. for Civ. Rights (Feb. 6, 2024), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (specifying Defendant as a HIPAA 'business associate' and the location of the breached Private Information as a 'network server').

[4] *MMRG Notifies Patients of Cybersecurity Incident, Business Wire* (Feb. 6, 2024), https://www.businesswire.com/news/beverlyhillschamber/20240206060527/en.

[5] *Id.*

[6] *Id.*

30. Upon information and belief, the Private Information stored and maintained by Defendant was not encrypted.

31. Upon information and belief, the targeted cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiff and the Class Members.

32. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as an entity that collects, creates, and maintains both PII and PHI.

33. Upon information and belief, Plaintiff's Private Information was accessed and stolen in the Data Breach.

34. Defendant informed impacted patients that they should take steps to monitor accounts and review credit statements.[7]

35. Further, Defendant offered to "qualified individuals" credit/identity monitoring services for two years.[8]

36. The offer of identity monitoring services is an acknowledgment by Defendant that the impacted customers are subject to an imminent threat of identity theft.

37. Despite discovering the Data Breach in November 2023 and acknowledging that data thieves likely accessed Plaintiff's and the Class Members' Private Information,

---

[7] *Id.*

[8] *Id.*

Defendant did not begin to notify affected customers until February 2024, nearly three months later.

38. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

39. Plaintiff and Class Members provided their Private Information to Defendant and/or its customers with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

40. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

41. In light of recent high profile data breaches at other healthcare companies, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

42. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because

they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

43. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Comply with FTC Guidelines

44. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

45. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[10] The guidelines also recommend that

---

[9] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), available at https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[10] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[11]

46. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

47. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. These FTC enforcement actions include actions against healthcare providers and business associates thereof like Defendant. See, e.g., In the Matter of Labmd, Inc., A Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were

---

[11] *Id.*

unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

49. Defendant failed to properly implement basic data security practices. Defendant failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

50. Defendant was at all times fully aware of its obligation to protect the PII and PHI of patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

51. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

52. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

53. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls ("CSC"), and all healthcare institutions are strongly advised to follow these actions. The

CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[12]

54. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

55. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are established standards in reasonable cybersecurity readiness.

---

[12] *See CIS Benchmarks FAQ*, Cent. for Internet Sec., available at https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/.

Defendant's Conduct Violates HIPAA and Evidences Their Insufficient Data Security

56. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

57. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

58. On the bottom of Defendant's website is a hyperlink titled "Privacy Policy." When a user clicks on "Privacy Policy," the user is taken to a webpage titled "Privacy Policy," which details individuals' privacy rights and the ways in which Defendant may use and share individuals' Private Information.[13]

59. Defendant's "Privacy Policy" page states that, "[f]or more information about these rights, please see the detailed Notice of Privacy Practices", yet this supposed "Notice of Privacy Practices" is nowhere to be found on the most updated version of Defendant's website.[14]

60. On a digitally archived version of Defendant's website with the "Notice of Privacy Practices" intact, the Notice provided the following:

> Your medical information is personal. American Vision Partners and all of their affiliates ("AVP") and its employees are dedicated to maintaining the privacy of your personal health information ("PHI"), as required by

---

[13] *Privacy Policy*, American Vision Partners, https://americanvisionpartners.com/privacy-policy/ (last accessed Feb. 29, 2024).

[14] *Id.*

> applicable federal and state laws. These laws require us to provide you with this Notice of Privacy Practices and to inform you of your rights and our obligations concerning PHI, which is information that identifies you and that relates to your physical or mental health condition. We are required to follow the privacy practices described below while this Notice is in effect.[15]

61. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

62. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S DUTY TO PLAINTIFF AND CLASS MEMBERS

63. Defendant breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

---

[15] *HIPAA Notice of Privacy Practices*, American Vision Partners (Oct. 1, 2020), https://web.archive.org/web/20230208043537/https://americanvisionpartners.com/notices/privacy-policy/.

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train their employees in the proper handling of PII and PHI;

f. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

p. Failing to adhere to industry standards for cybersecurity.

64. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

THE CONSEQUENCES OF DEFENDANT'S FAILURES

65. Cyberattacks and data breaches on medical facilities and technology vendors like Defendant are problematic because of the increased risk of fraud and identity theft.

66. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

67. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities in order to engage in illegal financial transactions

[16] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007), available at https://www.gao.gov/new.items/d07737.pdf.

under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

68. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

69. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

70. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical

---

[17] *See IdentityTheft.gov*, Fed. Trade Comm'n, available at https://www.identitytheft.gov/Steps .

services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

71. Moreover, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[18]

72. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

73. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[19]

74. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data

---

[18] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[19] *See Medical Identity Theft*, Fed. Trade Comm'n, available at http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 5, 2023).

breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

75. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

76. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

77. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

78. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

79. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

80. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[20] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

81. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[21] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[22] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

82. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may

---

[20] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), available at https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[21] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 5, 2023).

[22] *Id* at 4.

not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

83. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[24]

84. Medical information is especially valuable to identity thieves.

85. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[25] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[26]

---

[23] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), available at http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[25] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), available at https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[26] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), available at https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

86. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

87. For this reason, Defendant knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

88. Plaintiff Charles Peterson has received eyecare treatment at an eyecare center in Arizona.

89. The eyecare center is a customer of Defendant's medically-related administrative, management, and technology services.[27]

90. To use Defendant's services, the eyecare center gives and entrusts Plaintiff's and Class Members' PII and PHI to Defendant.

91. Plaintiff received a letter from Defendant, dated February 27, 2024, notifying Plaintiff that his Private Information may have been compromised in the Data Breach.

---

[27] *Our Practices*, American Vision Partners, https://americanvisionpartners.com/about/our-practices/ (last accessed Feb. 29, 2024) (listing Plaintiff's eyecare center as one of the ophthalmology practices serviced by Defendant).

92. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

93. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

94. After the Data Breach occurred, Plaintiff experienced substantial stress and anxiety worrying about the effects of the Data Breach and the impact it will have on his Private Information.

95. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

96. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

97. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

98. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

99. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

100. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

101. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach.

102. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiff and Class Members about all the time that they will need to spend monitor their own accounts, or to establish a security freeze on their credit report.

103. Upon information and belief, Plaintiff has spent several hours dealing with the consequences of the Data Breach, the time of which has included researching the details of the Data Breach, speaking with his bank and/or credit card companies to dispute fraudulent transactions, and determining the legitimacy of phone calls that may be spam.

104. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled, and;

k. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

105. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents

containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

106. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

107. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

CLASS ALLEGATIONS

108. Plaintiff brings this Action as a class action under Federal Rule of Civil Procedure 23 and seeks certification of the following nationwide Class ("Class"):

> All persons whose Private Information was accessed, compromised, copied, stolen, and/or revealed as a result of Defendant Medical Management Resource Group, LLC's Data Breach.

109. Excluded from the Class are Defendant, its officers and directors, and members of their immediate families or their legal representatives, heirs, successors or assigns and any entity in which Defendant has or had a controlling interest.

110. Class certification of Plaintiff's claims is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis utilizing the same evidence as would be used to prove those elements in separate actions alleging the same claims.

111. Numerosity—Federal Rule of Civil Procedure 23(a)(1). The Members of the Class are so numerous that joinder of all Class Members would be impracticable. Upon information and belief, the Class numbers in the millions. Also, the Class is comprised of an easily ascertainable set of patients who were impacted by the Data Breach. The exact number of Class Members can be confirmed through discovery, which includes Defendant's records. The resolution of Plaintiff's and Class Members' claims through a class action will behoove the Parties and this Court.

112. Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of fact and law exist as to all Members of the Class and predominate over questions affecting only individual Class Members. These common questions of law or fact, include, among other things:

a. Whether Defendant's cybersecurity systems and/or protocols before and during the Data Breach complied with relevant data security laws and industry standards;

b. Whether Defendant properly implemented their purported security measures to safeguard Plaintiff's and Class Members' private information from unauthorized access, propagation, and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the Data Breach after they first discovered the same;

d. Whether Defendant disclosed Plaintiff's and Class Members' private information in contravention of the understanding that the information was being revealed in confidence and should be maintained;

e. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures and security controls to preclude unauthorized access to Plaintiff's and the Class Members' private information;

f. Whether Defendant was unjustly enriched by their actions; and

g. Whether Plaintiff and Class Members are entitled to damages, injunctive relief, or other equitable relief, and the extent of such damages and relief.

113. Defendant engaged in a common course of conduct granting rise to the legal rights sought to be enforced by Plaintiff, on behalf of themselves and other Members of the Class. Similar or identical common law violations, business practices, and injuries are involved.

114. Typicality—Federal Rule of Civil Procedure 23(a)(3). Plaintiff's claims are typical of the claims of the other Members of the Class because, inter alia, all Class Members were similarly injured and sustained similar monetary and economic injuries as a result of Defendant's misconduct described herein and were accordingly subject to the alleged Data Breach. Also, there are no defenses available to Defendant that are unique to Plaintiff.

115. Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent, he retained counsel competent and

experienced in complex class action litigation, and he will prosecute this action earnestly. The Class's interests will be fairly and adequately protected by Plaintiff and their counsel.

116. Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2). Defendant acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate regarding the Class under Federal Rule of Civil Procedure 23(b)(2).

117. Superiority—Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

118. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications establishing conflicting standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class Members would create a risk of adjudication that would be dispositive of the interests of other Class Members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and

c. Defendant has acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief regarding the Members of the Class as a whole.

119. Class certification is also appropriate because this Court can designate specific claims or issues or class-wise treatment and may designate multiple subclasses under Federal Rule of Civil Procedure 23(c)(4).

120. No unusual difficulties are likely to be encountered in the management of this action as a class action.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

121. Plaintiff re-alleges and incorporate by reference paragraphs 1 through 120 above as if fully set forth herein.

122. In order to receive medical treatments and services, customers of Defendant required Plaintiff and Class Members to submit non-public Private Information, such as PII and PHI.

123. Plaintiff and Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their information.

124. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

125. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

126. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customer's patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

127. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

128. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

129. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

130. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

131. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

d. Failing to adequately train its employees to recognize and contain phishing attacks;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

g. Failing to timely notify Class Members about the Data Breach regarding what type of Private Information had been compromised so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

132. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

133. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

134. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

135. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit and identity monitoring to all Class Members.

136. Further, pursuant to HIPAA (42 U.S.C. § 1302d et seq.), the FTCA, and Nevada law, Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.

137. Plaintiff and Class Members are within the class of persons that the HIPAA was intended to protect.

138. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class.

139. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

140. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

141. Defendant breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

142. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendant's networks and computers that stored or contained Plaintiff's and Class Members' Personal Information.

143. Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to Defendant's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

144. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek damages and other relief as a result of Defendant's negligence.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

145. Plaintiff re-alleges and incorporate by reference paragraphs 1 through 120 above as if fully set forth herein.

146. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of medically-related administrative services, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

147. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when they first went for medical care and treatment at one of Defendant's customers' facilities.

148. The valid and enforceable implied contracts to provide medical health care services that Plaintiff and Class Members entered into with Defendant and/or its customers include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

149. When Plaintiff and Class Members provided their Private Information to Defendant and/or its customers in exchange for medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

150. Defendant and/or its agents solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

151. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with

relevant laws and regulations, including HIPAA, and were consistent with industry standards.

152. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

153. Under the implied contracts, Defendant and/or its customers promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: (i) provided to obtain such health care; and/or (ii) created as a result of providing such health care. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

154. Both the provision of medical services healthcare and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

155. The implied contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents.

156. Defendant's express representations memorialize and embody the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

157. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To patients such as Plaintiff and Class Members, healthcare services that do not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and/or its customers and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

158. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or its Agents, and paid for the provided healthcare services in exchange for, amongst other things, both the provision of health care and medical services and the protection of their Private Information.

159. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

160. Defendant materially breached its contractual obligation to protect the non-public Private Information Defendant gathered when the sensitive information was accessed by unauthorized personnel as part of the Data Breach.

161. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and approximately 2.4 million Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

162. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

163. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received health care and other medical services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the health care they received.

164. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

165. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering

additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

166. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

167. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

168. Plaintiff re-alleges and incorporate by reference paragraphs 1 through 120 above as if fully set forth herein.

169. This count is plead in the alternative to the breach of contract counts above.

170. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its customers and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

171. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

172. The amount Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

173. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

174. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

175. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

176. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to Defendant's services.

177. Plaintiff and Class Members have no adequate remedy at law.

178. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the

actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

179. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

180. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Classes)

181. Plaintiff re-alleges and incorporate by reference paragraphs 1 through 120 above as if fully set forth herein.

182. At all times during Plaintiff's and Class Members' interactions with Defendant and/or its customers, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information.

183. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

184. Plaintiff and Class Members provided their Private Information to Defendant and/or its Agents with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

185. Plaintiff and Class Members also provided their Private Information to Defendant and/or its customers with the explicit and implicit understandings that Defendant would take precautions to protect such Private Information from unauthorized disclosure.

186. Defendant voluntarily received in confidence Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

187. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

188. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

189. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their protected Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected Private Information, as well as the resulting damages.

190. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information.

191. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from medical fraud, financial fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of patients in their continued possession; and (viii) future costs in terms of time, effort, and money that will

be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

192. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

193. Plaintiff re-alleges and incorporate by reference paragraphs 1 through 120 above as if fully set forth herein.

194. In light of the special relationship between Defendant and its customers' patients, whereby Defendant became a guardian of Plaintiff's and Class Members' highly sensitive, confidential, personal, financial information, and other Private Information, Defendant was a fiduciary, created by its undertaking and guardianship of the PHI, to act primarily for the benefit of its customers' patients, including Plaintiff and Class Members, for: (1) the safeguarding of Plaintiff's and Class Members' Private Information; (2) timely notifying Plaintiff and Class Members of a data breach or disclosure; and (3) maintaining complete and accurate records of what and where Defendant's customers' patients' information was and is stored.

195. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its customers' patients' relationship, in particular to keep secure the Private Information of its customers' patients.

196. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently investigate the Data Breach to determine the number of Members affected in a reasonable and practicable period of time.

197. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect Plaintiff's and Class Members' Private Information.

198. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

199. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

200. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

201. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

202. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the

extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

203. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

204. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

205. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94).

206. Defendant breached its fiduciary duties to Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, et seq.

207. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to

mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of consumers/patients and former consumers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

208. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
Violation of the Arizona Consumer Fraud Act
A.R.S. §§ 44-1521, *et seq.* ("ACFA")
(On Behalf of Plaintiff and the Class)

209. Plaintiff re-alleges and incorporate by reference paragraphs 1 through 120 above as if fully set forth herein.

210. The ACFA provides the following:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation,

> or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

A.R.S. § 44-1521(A).

211. Plaintiff, Class Members, and Defendant are "persons" under the ACFA. A.R.S. § 44-1521(6).

212. The services provided by Defendant are "merchandise" under the ACFA. A.R.S. § 44-1521(5).

213. Defendant represented to its patients that their PII and PHI will remain private, as shown by its Privacy Notice.

214. Defendant engaged in unlawful practices in contravention of the ACFA by failing to implement and maintain reasonable security measures to secure its patients' PII/PHI in a manner compliant with applicable laws, regulations, and industry standards and failing to inform Plaintiff and Class Members that it would not adequately protect their PII/PHI. Instead, it made misrepresentations that Plaintiff's and Class Members' PII/PHI would be adequately protected.

215. As a result of the Data Breach, Plaintiff and Class Members have lost property in the form of their PII/PHI. Further, Defendant's failure to adopt reasonable practices in protecting and safeguarding its patients' PII/PHI will force Plaintiff and Class Members to spend time or money to protect against identity theft. Plaintiff and Class Members are now at a higher risk of medical identity theft and other crimes. This harm

sufficiently outweighs any justifications or motives for Plaintiff's practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

216. Plaintiff and all other Class members were damaged by Defendant's contravention of the ACFA because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT VII
Declaratory Judgment / Injunctive Relief
(On Behalf of Plaintiff and the Class)

217. Plaintiff re-alleges and incorporate by reference paragraphs 1 through 120 above as if fully set forth herein.

218. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

219. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that Defendant's data security measures remain inadequate.

220. Defendant has characterized the cybersecurity incident as "network security incident," targeted at Defendant's systems containing PII and PHI of Plaintiff and Class Members. The cybersecurity incident involved individuals' names, contact information, dates of birth, certain medical information, Social Security numbers and insurance information.

221. Defendant's November 2023 cybersecurity incident demonstrates the need for injunctive relief for Plaintiff and Class Members. Defendant has not implemented measures to protect Private Information, leaving Plaintiff and Class Members without a way of protecting themselves.

222. Plaintiff continues to suffer injuries as result of the compromise of his Private Information and remain at imminent risk that further compromises of his Private Information will occur in the future.

223. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (a) Defendant owes a legal duty to secure Plaintiff's and Class Members' Private Information, and to timely notify impacted individuals of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes, and (b) Defendant continues to breach this legal

duty by failing to employ reasonable measures to secure Private Information in its possession.

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

c. prohibiting Defendant from engaging in the wrongful and unlawful acts alleged herein;

d. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

e. requiring Defendant to delete and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

f. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;

g. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. prohibiting Defendant from maintaining Plaintiff's and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

i. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

j. requiring Defendant to conduct regular database scanning and securing checks;

k. requiring Defendant to monitor ingress and egress of all network traffic;

l. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiff and Class Members;

m. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

n. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring

tools are properly configured, tested, and updated; and

o. requiring Defendant to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

224. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at, or implicating, Defendant. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

225. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

226. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: March 1, 2024

Respectfully submitted,

/s/ Elaine A. Ryan
Elaine A. Ryan (AZ Bar No. 012870)
Colleen M. Auer (AZ Bar No. 014637)
AUER RYAN, P.C.
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139
(520) 705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com

Jean S. Martin*
North Carolina Bar No. 25703
Francesca K. Burne*
Florida Bar No. 1021991
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jeanmartin@forthepeople.com
fburne@forthepeople.com

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class